



ROB S. SAXTON
Deputy Superintendent of Public Instruction

HB 4062: Privacy of Student Records
House Education Committee
Jan McComb & Doug Kosty
February 3, 2014

Good afternoon Chair Gelser and members of the House Education Committee. For the record, I am Jan McComb speaking on behalf of the Oregon Education Department. I am here today with Doug Kosty, our Assistant Superintendent in the Office of Learning. We are here today to speak about HB 4062.

Background

The safety, accuracy, and security of student education records is a critically important mission for the Oregon Department of Education. ODE has created a comprehensive Information Security and Privacy Program that incorporates security at all the different levels of student data and personal information.

ODE is required by law to collect and store student educational records and have done so for more than a decade; we've not experienced a single breach or exposure of personally identifiable information in that time. The department follows state information security laws and the federal Family Educational Rights and Privacy Act (FERPA). As a state agency, ODE is also subject to the Department of Administrative Services' Enterprise Security Office which institutes security measures to protect information maintained by the state.

There are three primary risks to student data: human error and misuse; unsound processes and policies; and technology failures.

To reduce the potential for human error, ODE provides annual mandatory information security and privacy fundamentals training; provides monthly security and privacy newsletters and security bulletins as needed; and provides targeted information security training for specific groups, such as Information Security and Privacy Training for district security administrators and special education collections coordinators.

To ensure ODE and schools are using the most up-to-date processes and policies, we monitor changes in state and federal regulations and update our policies in response. FERPA was recently reauthorized to include additional clarity around the construction and use of statewide longitudinal data systems, for instance. ODE has created a number of policies around this issue, including the acceptable use of personally identifiable student information. ODE conducts security audits against systems to make sure access and rights are appropriate and conducts security reviews of any procurements and contracts involving data exchange, data access, and research.

The technology element focuses on technologies that support the protection of the confidentiality, integrity, and availability of the data and the systems we are responsible for securing. A short list of the security measures taken to protect student data include encryption of data, firewalls, limited access to data, and backup and offsite secure storage.

In addition to maintaining a comprehensive Information Security and Privacy Program for the department, ODE launched a statewide Education Information Security Council, in partnership with school districts and ESDs.

Issue

How to best maintain the privacy of student education records?

Legislation

HB 4062 seeks to strengthen the state's security laws concerning student education records and reduce the risk that student information is misused by shortening the timeline in which it exists; allowing that data be corrected by parents or students who have turned 18; and eliminating the use of student data for any purpose that does not directly benefit the student, educationally. It also directs ODE to provide technical assistance to school districts in complying with student education records law and directs the department to "issue a privacy risk assessment of any data system, program, or contract involving student education records."

With reports of information security breaches in the news, the department appreciates and supports the intent behind this legislation. Many of the ideas contained in HB 4062 seem quite reasonable and in some cases are already law. However, a number of provisions would have consequences that are not immediately obvious. Below are some highlights.

(3)(d) Require that personal identifying information collected about a student and retained in the student education record be only used for the educational benefit of the student. This provision violates federal law (34 C.F.R. § 99.36 (2012)) as it prohibits school personnel from disclosing student information to law enforcement in a student health and safety emergency (e.g. missing child). ODE gets data requests based on Amber Alerts about once a month from the state police. This same section would prohibit the creation of longitudinal data bases and could potentially cost ODE millions in grant funds, and violates Oregon's waiver from federal *No Child Left Behind* act requirements as the state pledged to create a longitudinal database, and hinders ODE and local districts from evaluating schools, districts, and programs.

(3)(f) Prohibit the disclosure of student personal identifying information to individuals who are not directly responsible for the student's education program. This provision would curtail the role of research in analyzing the overall success of education programs. This could significantly impact the ability of ODE and OEIB to evaluate the success of initiatives and programs to support the 40-40-20 goal. As written, it is more restrictive than FERPA which specifically allows for the use of student data in education research. HB 4062 may prohibit the ability of ODE or districts to compete for grant funding that requires student-level data and analysis. Also, because ODE and school districts and ESDs use the same student identifying system, this prohibition could result in either ODE or school districts and ESDs changing or abandoning the student identifying system and creating new, idiosyncratic

systems that vary from district to district, or returning to the use of social security numbers, which were discontinued due to identify theft concerns.

(3)(g) Prohibiting the collection of student personal identifying information for general educational research or program evaluation purposes. Many federal grant programs require that educators track how well the program succeeded in better educating students, and require evidence of this. This provision could prevent the state from receiving federal grants as we would not be able to provide the data for accountability purposes. The many “strategic initiatives” enacted by the 2013 Legislature all require reports on their respective successes. This provision could prevent that data from being collected. This section would potentially cost the state millions in grant funds and it violates Oregon’s waiver from federal Elementary and Secondary Education Act requirements.

(3)(i) Require that student personal identifying information be removed from the student education record when the student personal identifying information is no longer needed for the purposes of preparing the student’s education program, application for employment or application to a post-secondary institution. This provision violates federal FERPA law and state public records law as it destroys part of the student record. It is also unclear at what point the record would be destroyed. Transcripts are often requested by adults who decide to go back to school at a later age. At what point would the student no longer need the information for a job? This could also affect the viability of the longitudinal data system to demonstrate return on investment in education across a timespan of more than a few years. ODE is often required to be able to demonstrate how published reports were generated and to respond to requests about the data. This requirement would inhibit ODE’s ability to reconstruct the reports and demonstrate the accuracy of the published work upon request.

(3)(j) Permit an educator or school administrator whose performance is evaluated using student information contained in a student education record to view the information used for purposes of the evaluation. The provision reduces student privacy and as worded may violate FERPA as this is not a specified allowable disclosure of student records. For example, a student’s status as homeless would not ordinarily be accessible by a teacher and may be something the student wishes to keep confidential.

(8) Using the standards adopted under this section as guidance, the department shall issue a privacy risk assessment of any data system, program, or contract involving student education records. The scope of this language is very broad and would be expensive to carry out. Using the definition in subsection (1) of the bill, those schools that would be subject to an ODE risk assessment would include private schools, over 1200 public schools, 19 ESDs, residential treatment programs, day treatment programs, detention facilities, and youth care centers. Also the words, “any data system, program, or contract involving student education records,” would potentially capture hundreds if not thousands, types of systems and programs and generate thousands of risk assessments.

Thank you for this opportunity to present some concerns of the Department of Education. ODE remains committed to student privacy. We would be happy to work with Rep. Frederick on refining the language in the bill.